Karakteristike sigurnosti Encrypting File System-a

Dragoljub Pilipović

***Sadržaj* — Dva standardna mehanizma zaštite podataka od neovlašćenih pristupa su kontrola pristupa korisnika i enkripcija odnosno šifrovanje. Tako operativni sistem dodeljuje korisniku prava zapisana u ACL listama, dok kriptografski sistem datoteka obezbeđuje sloj zaštite za podatke u onim slučajevima kada kontrola pristupa nije aktivna. Podaci koji nemaju zaštitu kontrole pristupa iz nekog razloga, mogu biti šifrovani te se njima može pristupiti samo uz posedovanje odgovarajućeg ključa dešifrovanja. U ovom radu se prezentuje New Technology File System (NTFS) i njegov deo Encrypting File System (EFS), koji predstavlja primer kombinacije mehanizama kontrole pristupa i šifrovanja.**

***Ključne reči* — EFS, šifrovanje, kontrola pristupa, NTFS, sigurnost.**

I. UVOD

NEW Technology File System (NTFS) predstavlja sistem datoteka opšte namene koji je uobičajen na Windows familiji operativnih sistema američke firme Majkrosoft. Njegovo prvo pojavljivanje je vezano uz Windows NT 3.1 iz 1993. godine. Verzije su vezane za pojedine verzije operativnih sistema, te je danas aktuelan NTFS sa verzijom 5.1 [1].

Aktuelni NTFS je visokoperformansni i samoobnovljivi sistem datoteka sa najvećim volumenom od 256 TiB, najvećom mogućom datotekom od 16 TiB, maksimalnim brojem datoteka od 2^{32}-1 i najvećom dužinom imena datoteke od 255 dvobajtnih Unicode znakova. Raspon mogućih datuma počinje od godine 1601. do godine 60056 [2]. Tačna specifikacija ovog sistema datoteka nije poznata, jer predstavlja komercijalnu tajnu.

Osnovna struktura jeste volumen zasnovan na logičkoj particiji diska, koja

D. Pilipović, Fakultet za informacione tehnologije, Slobomir P Univerzitet, 76300 Bijeljina, Republika Srpska, BiH; (e-mail: dragoljub.pilipovic@gmail.com).

može zauzeti deo diska, ceo disk a može se rasprostirati na više diskova. Interno, podseća na bazu podataka koja organizuje podatke po principu B+ stabla [3]. Sistemsko zapisivanje u dnevnik garantuje integritet sistema datoteka, ali ne i samog sadržaja pojedinih datoteka.

Neki mehanizmi zaštite Windows operativnog sistema su autentifikacija korisnika pri log-on procesu, kontrola pristupa na nivou sistema datoteka i kriptografske mere zaštite [4]. Kontrola pristupa korisnika se nadgleda za objekte sistema datoteka (datoteke i direktorijume) preko ACL (Access Control List) listi. Liste određuju koji korisnik ili grupa korisnika može da pristupi nekoj određenoj datoteci/direktorijumu i šta od dozvola ima omogućeno ili zabranjeno. Ovaj rad će se fokusirati na kriptograski deo NTFS-a.

II. ENCRYPTING FILE SYSTEM

Od verzije 5.0, NTFS ima mogućnost disk šifrovanja objekata sistema datoteka putem Encrypting File System-a (EFS) [1]. Postoje dve generalne vrste disk šifrovanja: one koje šifruju celi disk i one koje šifruju pojedine objekte sistema datoteka poput datoteka i direktorijuma. U ovaj drugi tip spada EFS.

Dok je operativni sistem u aktivnom stanju (tj. operativni sistem je pokrenut i izvršava se u radnoj memoriji i na centralnom procesoru), kontrola pristupa korisnika pruža dovoljno sigurnosti za objekte sistema datoteke uz pretpostavku adekvatne upotrebe njenih mogućnosti. Međutim, kada operativni sistem nije aktivan ili je aktivan onaj koji nije iz Windows familije, onda kontrola pristupa preko ACL liste može biti zaobiđena. Šifrovanje datoteka i direktorijuma pruža poverljivost odnosno privatnost pristupa podacima koji se nalaze na sistemu datoteka [5].

Takođe, EFS čuva sadržaj datoteka od uljeza koji bi mogli steći fizički pristup kritičnim podacima (na primer, krađom prenosnih računara ili spoljnog diska).

Šifrovanje putem EFS-a nije dovoljna da obezbedi jedan od sigurnosnih ciljeva CIA trojke, integritet, jer ne može da sprečiti nekog napadača da obriše šifrovanu datoteku i na taj način izvrši neautorizovanu modifikaciju. Prema tome, disk šifrovanje predstavlja još jedan dodatni sloj u zaštiti podataka.

EFS ima sledeće prednosti u odnosu na korišćenje drugih aplikacija za šifrovanje datotečnih sistema [6]:

- Transparentnost. Transparentan je za korisnike i za sve aplikacije. Jednom kada je datoteka ili direktorijum označen kao šifrovan, biće šifrovan

u pozadini bez interakcije sa korisnikom. Korisnik ne mora da pamti neku lozinku da bi dešifrovao podatke.

- Jaka sigurnost. Koriste se standardni kriptografski algoritmi poput DES-X, 3DES i AES sa poznatim ranjivostima, manama i prednostima.
- Zaštita procesa (de)šifrovanja. Svi (de)šifrujući procesi se izvode u zaštićenom režimu rada operativnog sistema.
- Mehanizam oporavka. EFS obezbeđuje mehanizam oporavka podataka koji je značajan u poslovnom okruženju, dajući organizaciji mogućnost da dođe do podataka, čak i ako je zaposleni koji ih je šifrovao napustio kompaniju.

III. ŠIFROVANJE I DEŠIFROVANJE EFS-A

Za uključivanje šifrovanja za neku datoteku ili direktorijum potrebno je uraditi jednu od sledećih akcija:

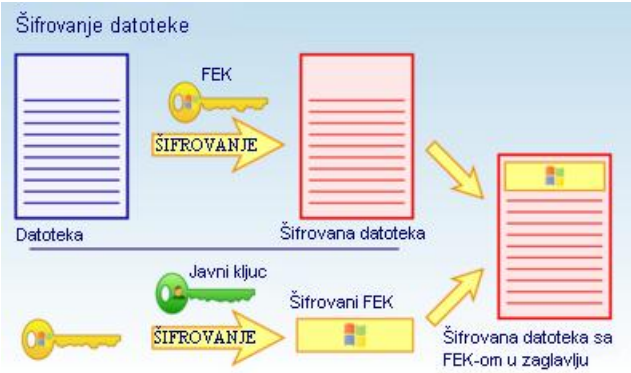
- U grafičkom režimu za izabrani objekat u njegovim svojstvima na dijalogu Advanced Attributes izabrati opciju Encrypt contents to secure data.
- Dodati objekat u već šifrovan direktorijum.
- U konzolnom režimu koristiti naredbu cipher.exe sa odgovarajućim parametrima.

Šifrovanje se isključuje na isti način, ali u suprotnom smeru.

EFS koristi kombinaciju simetričnog i asimetričnog načina šifrovanja. Simetrični ključ šifrovanja (FEK, File Encryption Key) se koristi za same podatke odnosno za pojedinačne datoteke. Par javnog i privatnog RSA ključa se koristi da bi zaštitio simetrični ključ. Razlog zašto se koriste dva različita načina je brzina procesa šifrovanja. Teret performansi asimetričnog šifrovanja je prevelik da bi se njime šifrovale velike količine podataka. Simetrični algoritmi su oko 100 do 1000 puta brži, što ih čini pogodnim za šifrovanje velikih količina podataka [6].

Proces šifrovanja jedne datoteke se sastoji od sledećih koraka (sl. 1.):

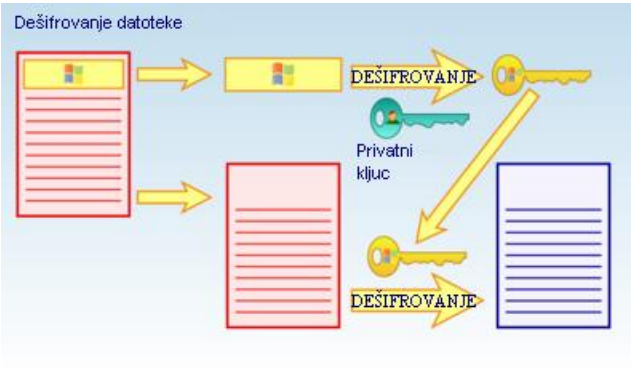
1. Operativni sistem pravi jedinstveni simetrični ključ FEK.
2. Koristeći FEK šifrira se polazna datoteka.
3. Korisnikov javni ključ će biti upotrebljen za šifrovanje FEK-a.
4. Konačna šifrovana datoteka se sastoji od šifrovanog FEK-a i šifrovane polazne datoteke.



Sl. 1. Proces EFS šifrovanja datoteke [2]

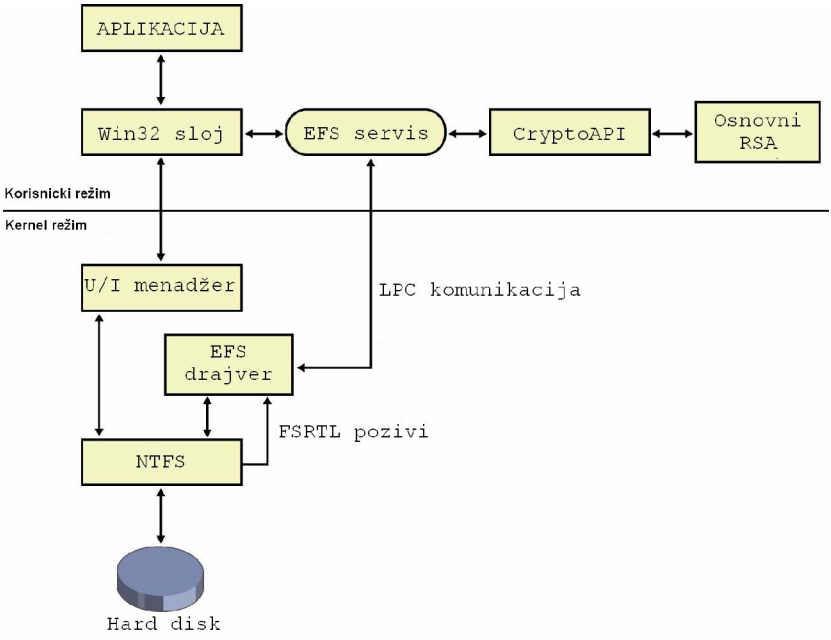
Obrnut proces za jednu šifrovanu datoteku se sastoji od sledećeg (sl. 2.):

1. Izdvajaju se šifrovani FEK i šifrovani podaci datoteke.
2. Pomoći korisnikovog tajnog ključa se izvodi dešifrovanje simetričnog ključa.
3. Sada se FEK koristi za simetrično dešifrovanje da bi se dobila polazna datoteka.



Sl. 2. Proces dešifrovanja EFS datoteke [2]

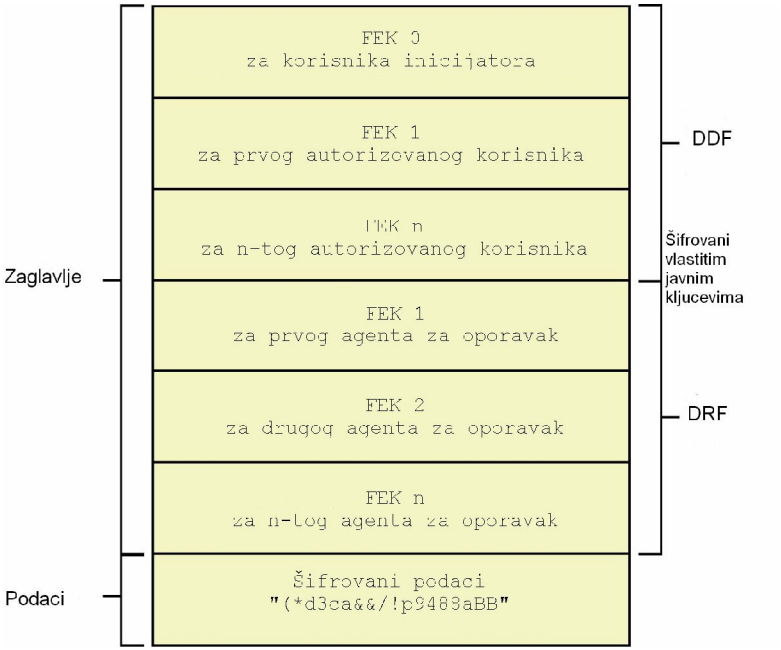
Kao prvi korak šifrovanja, NTFS kreira log datoteku po imenu Efs0.log u direktorijumu System Volume Information na istom disku gde je i datoteka. Onda EFS dobija pristup CryptoAPI kontekstu. Uz pomoć njega, EFS generiše FEK.



Sl. 3. Arhitektura EFS-a [1]

Sledeći korak se sastoji u dobijanju javnog/privatnog para ključeva; ako ne postoji u ovoj fazi (slučaj kada je EFS upotrebljen po prvi put), EFS generiše novi par. EFS koristi RSA algoritam da šifruje FEK.

Onda EFS kreira DDF (Data Decryption Field) za trenutnog korisnika tj. za onog koji je pokrenuo proces šifrovanja, gde postavlja FEK i šifruje ga sa javnim ključem. Ako je agent za oporavaka (recovery agent) definisan sistemskom politikom, EFS takođe kreira DRF (Data Recovery Field) i tu postavlja FEK šifrovan sa javnim ključem agenta. Poseban DRA je kreiran za svakog definisanog agenta za oporavak. Ako postoje korisnici koji imaju pravo na istu datoteku, onda se još pravi odgovarajući broj DDF polja sa šifrovanim FEK ključem na isti način, sa pripadajućim javnim ključevima. Na kraju se dobija struktura podataka kao na sl. 4.



Sl. 4.Sadržaj šifrovanog objekta sistema datoteka [1]

Sada je Efs0.tmp kreiran u istom direktorijumu u kojem se nalazi datoteka za šifrovanje. Sadržaj originalne datoteke (plain text) je kopiran na privremeno mesto, te je posle toga original zamenjen šifrovanim podacima. Nakon završenog šifrovanja, privremene i log datoteke su izbrisane.

Nakon što je datoteka šifrovana, samo korisnici koji imaju odgovarajući DDF ili DRF mogu pristupiti datoteci. Ovaj mehanizam je odvojen ali i uporedan sa uobičajenom kontrolom pristupa putem ACL listi koji se podrazumevano koristi. Samo korisnik koji može dešifrovati FEK sa svojim privatnim ključem, može pristupiti podacima.

Prvo operativni sistem proverava da li korisnik ima privatni ključ koji koristi EFS. Ako ima, on čita EFS atribute i ide kroz DDF polja tražeći DDF za trenutnog korisnika. Ako je DDF pronađen, koristi se korisnikov privatni ključ da dešifruje FEK izdvojen iz DDF polja. Koristeći dešifrovani FEK, EFS dešifruje sadržaj datoteke i njega isporučuje aplikaciji koja ga dalje koristi.

FEK nastaje preko generatora slučajnih brojeva i jedinstven je za datoteku. EFS dobija FEK iz statički povezane biblioteke koja ne može biti zamenjena nekom drugom.

Pošto simetrično šifriranje ne povećava količinu procesiranih podataka, veličina novostvorene datoteke tako se povećava u minimalnom iznosu. Veličina datoteke izražena u KiB ili većim jedinicama je najčešće ista pre šifrovanja i posle šifrovanja.

IV. KRIPTOGRAFSKI ALGORITMI U EFS-U

U EFS-u se koriste razni kriptografski algoritmi i tehnike, poput DES-X, 3DES, AES, RSA, RC4 i jednosmernih hash funkcija.

NTFS 5.0 u Windows 2000 operativnom sistemu koristi jedino DES-X kao simetrični algoritam, NTFS 5.1 kod Windows XP Proffesional-a alternativno može da koristi 3DES, dok je ista verzija ako ima Service Pack 1 instaliran sposobna da koristi kao treći algoritam i AES-256 (kao i sve Server 2003 i Vista ne-kućne verzije).

EFS koristi bazu podataka Registry da odluči koji će simetrični algoritam koristiti od raspoloživih. Ako je vrednost HKLM \ System \ CurrentControlSet \ Control \ Lsa \ FipsAlgorithmPolicy = 1, onda se koristi 3DES [1]. A ako ne, onda EFS proverava HKLM \ Software \ Microsoft \ Windows NT \ CurrentVersion \ EFS \ AlgorithmID (ovaj ključ ne mora biti prisutan). Podešavanje da bi podrazumevani simetrični algoritam bio 3DES je izvodljivo iz gpedit.msc konzole na putanji Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Security Options i politici `System cryptography: Use FIPS compliant algorithms for encryption`.

FIPS (Federal Information Processing Standards) broj 140-1 je standard koji govori o sigurnosnim zahtevima za kriptografske module, izdat od strane američkog NIST-a (National Institute of Standards and Technology). Algoritam trostrukog DES-a (Triple DES, 3DES) je saglasan sa FIPS 140-1 objavom standarda [7].

DES-X je manje poznati simetrični algoritam i predstavlja varijaciju DES algoritma, predhodnog standarda vlade SAD-a. Kao što je poznato da DES nije otporan na napade tzv. grubom silom (brute-force attack) zbog male veličine ključa od 56 bita, sa DES-X se probalo popraviti stanje bez značajnijih zahvata u osnovnom pristupu. Predložio ga je Ron Rivest 1984. godine, po sledećoj formuli:

$$\text{DES-X}(M) = K_2 \oplus \text{DES}_K(M \oplus K_1)$$

gde su M podaci za šifrovanje, K_1 i K_2 dodatni ključevi oba dužine 64 bita a između se koristi operacija ekskluzivnog ILI.

CryptoAPI je uobičajeno ime za Microsoft Cryptographic API, koji obezbeđuje interfejs ka svim kriptografskim operacijama koje zahteva EFS. Podržava i simetrični način kriptografije kao i kriptografiju javnim ključem. Neke od dostupnih operacija su: kreiranje ključeva, razmena ključeva, šifrovanje, dešifrovanje, hashing, digitalno potpisivanje, sigurni kriptografski pseudoslučajni generator brojeva.

CryptoAPI radi u sprezi sa različitim kriptografskim servisima (CSP, Cryptographic Service Providers) koji su instalirana na operativnom sistemu. CSP-ovi predstavljaju module koji rade stvarni deo šifrovanja i dešifrovanja. Od samog Majkrosofta su instalirani Basic, Enhanced i Strong servisi.

FSRTL (File System Run-Time Library) je deo EFS upravljačkog programa koji omogućuje otvaranje, čitanje i pisanje za šifrovane datoteke i direktorijume.

V. MEHANIZAM OPORAVKA KOD EFS-A

Proces obnavljanja odnosno oporavka (recovery) je sličan dešifrovanju, osim što koristi privatni ključ agenta za oporavak da bi se dešifrovao FEK u DRF, ne u DDF polju. Korisnički nalog koji je vezan za sertifikat agenta za oporavak će izvršiti dešifrovanje datoteke.

Kada neki korisnik postavi enkripcioni atribut za objekat sistema datoteka, EFS će prvo pokušati pronaći sertifikat korisnika u njegovom ličnom spremištu sertifikata. Ako takav ne postoji, onda će EFS isti zatražiti od organizacijskog sertifakacionog tela (CA, certificate authority). Ako i takav ne postoji, EFS će automatski generisati samo-potpisani sertifikat za tog korisnika.

U bilo kojem slučaju, javno-privatni par ključeva će se zahtevati od CryproAPI-ja. Javni ključ se nalazi u ličnom spremištu sertifikata dok se privatni ključ nalazi u korisničkom profilu. Korisnički profil je struktura direktorijuma i datoteka koji pripadaju nekom određenom korisniku i nosi najveći deo podataka tog korisnika.

Korisnički digitalni sertifikat je stalno smešten na sledećoj putanji: %USERPROFILE% \ ApplicationData \ Microsoft \ SystemCertificates \ My \ Certificates za svakog korisnika, gde je %USERPROFILE% sistemska promenljiva. Sa tog mesta sertifikat se, svaki put kad se korisnik prijavi na sistem, prebacuje u lično spremište sertifikata. Za korisnike koji imaju lutajući (roaming) tip profila, sertifikat se nalazi u Active Directory bazi podataka domenskog kontrolera te na taj način prati korisnika kada se on loguje na bilo koji računar u domenu. Sadržaj ličnog spremišta sertifikata se može pogledati u certmgr.msc konzoli na putanji Personal \ Certificates. U polju Intend Purpose za korisnike stoji Encrypting File System, a za agenta

oporavka stoji File Recovery. Sertifikat agenta za oporavak se može videti u i gpedit.msc konzoli na putanji Local Computer Policy \ Computer Configuration \ Windows Settings \ Security Settings \ Public Key Policies \ Encrypting File System, odakle se može pokrenuti akcija Add Data Recovery Agent.

Sertifikati se nalazu u formatu X.509 verzija 3, javni RSA ključ je dužine 1024 bita a za digitalno potpisivanje se koristi hash algoritam SHA-1.

Postojanje agenta za oporavak zavisi od verzija operativnog sistema i njihovog okruženja. Tako na samostalnom Windows XP Professional sistemu ne postoji podrazumevani agent po instaliranju sistema od nule, na Windows Server 2003 on postoji, dok je za članove domena podrazumevani onaj koji je definisan grupnim politikama domena.

Radi pojačanja sigurnosti preporučljivo je arhivirati informacije kao što su ključevi, potpisi i sertifikati. U operativnom sistemi Windows se koristi više formata za ove potrebe, a najčešći su .cer i .pfx.

Format .cer sadrži digitalni sertifikat po X.509 propisu zapisanog u DER ili Base64 kodu. S druge strane, format .pfx sadrži sertifikat kao i privatni ključ, a može sadržati više sertifikata ili čak neophodan lanac sertifikata. Baziran je na RSA propisu PKCS #12 (Public Key Cryptografy Standards) [8].

Sertifikati i privatni ključevi se mogu eksportovati u ove datoteke iz ličnog spremišta sertifikata sa opcijom Export ili iz komandne linije sa cipher.exe naredbom uz upotrebu /r parametra. U prvom slučaju biramo da li nam treba samo sertifikat, te dobijamo .cer datoteku, ili nam treba i privatni ključ, te dobijamo .pfx datoteku. Privatni ključ se može zaštiti lozinkom i, posle uspešnog izdvajanja, obrisati iz spremišta. U drugom slučaju ako radimo sa komandnom linijom dobijamo obe datoteke.

Te datoteke se čuvaju u skladu sa sigurnosnom politikom organizacije, npr. u sefu na prenosivim memorijskim medijumima. Kada dođe trenutak za oporavak, potrebno je sertifikate i privatne ključeve upotrebiti iz ličnog spremišta, gde se oni mogu smestiti ili jednostavnim pokretanjem dotičnih datoteke ili sa opcijom Import iz spremišta. Potrebno je izabrati automatsko smeštanje ili ručno ih smestiti u Personal spremište.

Sistemski servis koji se brine da ne dođe do neautorizovanog pristupa privatnim ključevima i drugim poverljivim informacijama od strane korisnika, procesa i drugih aplikacija se identifikuje kao Protected Storage servis u services.msc konzoli a u Task Manager-u kao lsass.exe proces. Ne može se ugasiti kao proces, a ako dođe do prestanka rada servisa sistem će se restartovati.

Postoji pet nivoa zaštite koje ima enkripcioni objekat koje transparentno obezbeđuje operativni sistem:

1. EFS koristi FEK ključ kojim štiti podatke objekta.
2. FEK ključ se štiti sa javnim ključem korisnika i agenata za oporavak.
3. Servis Protected Storage upotrebljava korisnikov tzv. master key da zaštiti njegov privatni ključ. Privatni ključevi koji će se koristiti za dešifrovanje se nalaze zaštićeni u %USERPROFILE% \ Application Data \ Microsoft \ Crypto \ RSA \ User SID direktorijumu.
4. Isti servis će generisati simetrični ključ izveden od korisnikovih akreditiva, uključujući lozinku, da bi zaštitio master key, te se smešta u %USERPROFILE% \ Application Data \ Microsoft \ Protect \ User SID direktorijum.
5. Dodatni nivo zaštite je tzv. system key koji može da zaštićuje sve korisničke master ključeve.

Uprkos naporima Windows-a da zaštiti ključeve, činjenica je da su sve informacije smeštene na lokalnom računaru, te daju šansu napadačima, koji su dobili pristup hard disku, da otkriju ključeve i da ih upotrebe za dešifrovanje zaštićenih podataka. Ukupna bezbednost bi mogla biti značajno povećana šifrovanjem privatnih ključeva pominjanim sistemskim ključem. Program syskey.exe služi da se uključi/isključi ova opcija. Sistemskim ključem se pored master ključa šifruju još i lozinke smeštene u lokalnu SAM bazu korisnika, korisnike u Active Directory bazi i ostale Local Security Authority informacije. Smešta se na hard disk te u tom slučaju nema dodatne interakcije sa korisnikom; ipak postoji mogućnost smeštanja na flopi disketu i na taj način potpunog uklananja sa računara. U tom slučaju korisnik mora da ubaci disketu sa sistemskim ključem kada se operativni sistem startuje. Ovu metodu treba koristiti oprezno iz razloga što, u slučaju gubitka diskete, nema načina za pristup. Još je moguće koristiti dodatnu lozinku pre logovanja, jer je iz nje izveden sistemski ključ.

VI. POTENCIJALNI PROBLEMI I REŠENJA

Privremena datoteka nije izbrisana [9]. Kada EFS šifruje datoteku, kopira njen sadržaj u privremenu skrivenu datoteku po imenu Efs0.tmp u istom tom direktorijumu. Zatim šifruje početni tekst po blokovima i upisuje šifrovane podatke u originalnu datoteku. Nakon tog procesa privremena datoteka je izbrisana. Problem je u tome što EFS jednostavo označava privremenu datoteka kao obrisanu, a ne briše je fizički sa diska, što čini mogući pristup nezaštićenim podacima veoma lakim koristeći neki od recovery softvera niskog nivoa. Rešenje – fizički obrisati slobodni prostor. Čak i ako je pisano preko početnog teksta, mali tragovi magneta ostaju i tako ostavljaju šansu za

čitanje obrisanih podataka uz korišćenje određene opreme. Da bi smanjili tu šansu, koristi se komanda cipher.exe /w koja će sav nealocirani prostor da sa tri prolaza prebriše. U prvom prolazu upisuje nule, u drugom jedinice a u trećem pseudoslučajni niz.

Imena datoteka u šifrovanim direktorijumima nisu zaštićena. Zapravo, šifrujući sadržaj direktorijuma automatski podrazumeva da se šifrovanje primenjuje na sve datoteke u direktorijumu, a ne na listu datoteka u direktorijumu. Pošto samo ime može sadržati osetljive informacije, to bi mogao biti sigurnosni propust. Jedno od rešenja bi bilo korišćenje šifrovanih .zip arhiva umesto direktorijuma, koje su u Windows-u tretirane skoro kao i direktorijumi. Na taj način dovoljno je da šifrujemo samo jednu datoteku da bi zaštitili sve podatke.

Posle reseta lozinke, ne može se pristupiti šifrovanim objektima. Kada korisnik ima potrebu za brisanjem (reset) lozinke, najčešće jer je zaboravljena, to će učiniti administrator. Ovo se takođe događa ako se koriste specijalni alati za brisanje lozinki npr. kada originalni operativni sistem nije aktivan ili dođe do upada sa mreže. Master key koji se koristi da bi zaštitio privatni ključ korisnika je zaštićen sa ključem koji je delom nastao od tada validne lozinke. Ako se lozinka mora obrisati, onda dolazi do toga da se korisnik može logovati, ali ne može uraditi dešifrovanje. Nema rešenja, ali postoji upozorenje kada se pokuša uraditi reset lozinke: "Resetting this password might cause irreversible loss of information for this user account. For security reasons, Windows protects certain information by making it impossible to access if the user's password is reset."

Istekao rok trajanja sertifikata. Iako se EFS sertifikati prave za 10 godina korišćenja, može doći do njihovog isteka. Rešenje – koristiti komandu cipher.exe /u.

Privremene radne datoteke nisu zaštićene. Pri korišćenju npr. Office Word-a, pravi se u direktorijumu gde je dokument koji se obrađuje, privremena datoteka koja nije šifrovana kao što je sam dokument. Rešenje – šifrovati celi direktorijum.

Pogrešno ili zlonamerno korišćenje. Rešenje – isključiti mogućnost šifrovanja.

Postoje još neki dodatni problemi kao što su nešifrovana virtuelna memorija, hiberacijski režim rada, podaci koji se štampaju, antivirusni program ne može pristupiti svim datotekama, što se ovde neće razmatrati.

VII. ZAKLJUČAK

U radu je opisan EFS, enkripcioni deo NTFS 5.1 sistema datoteka. Šifrovanje, koliko da ima mnogo prednosti, ima i određene mane, te treba biti oprezan pri upotrebi.

Windows verzije 6 (Vista) donosi određene novine kao što upotreba sertifikata sa smart kartica, šifrovanje datoteke za straničenje pagefile.sys, šifrovanje celog diska nazvanu BitLocker.

LITERATURA

[1] Microsoft TechNet, www.microsoft.com, ključna reč za pretragu "efs", januar 2009.
[2] Wikipedia-the free encyclopedia, www.wikipedia.org, ključna reč za pretragu "nfts", januar 2009.
[3] B. Đorđević, D. Pleskonjić, N. Maček, "Operativni sistemi", Mikro knjiga, Beograd, 2005.
[4] D. Pleskonjić, B. Đorđević, N. Maček, M. Carić, "Sigurnost računarskih mreža", Viša elektrotehnička škola, Beograd, 2006.
[5] X. Zhou, "Steganographic File System", PhD Thesis, Department Of Computer Science, School Of Computing, National University Of Singapore, 2005.
[6] A. Matić, "NTFS – New Tehnology File System", seminarski rad, Slobomir P Univerzitet, Bijeljina, 2008.
[7] National Institute of Standard and Technology, www.nist.gov, ključna reč za pretragu "fips", janaur 2009.
[8] RSA Data Security Inc, www.rsa.com, ključna reč za pretragu "pkcs", januar 2009.
[9] www.ntfs.com, januar 2009.
[10] A. Ruth, K. Hudson, "Sertifikat Security+", CET, Beograd, 2004.

ABSTRACT

User access control and encryption are standard mechanisms for protecting data from unauthorized accesses. The operating system grants user accesses according to his specifications from ACL's, while cryptographic files systems provide a layer of protection for data when access control is unavailable. When data leaves the protection of access control, it can be encrypted when that it is only accessible to those who are assigned decryption keys. In this paper, we presented New Technology File System (NTFS) and its part, Encrypting File System (EFS), which is example that combines the mechanisms of access control and encryption.

SECURITY CHARACTERISTICS OF ENCRYPTING FILE SYSTEM

Dragoljub Pilipović